AMENDMENTS TO THE SPECIFICATION

Please amend the paragraph beginning on page 10, line 4 as follows:

Tatsuaki Okamoto, "Generic conversions for constructing IND-CCA2 public-key encryption in the random oracle model", online, The 5th Workshop on Elliptic Curve Cryptography (ECC 2001), October 30, 2001 ~~(retrieved on September 29, 2002 on the Internet in the following address: <www.cacr.math.uwaterloo.ca/conferences/2001/ecc/okamoto.ppt>~~

Please amend the paragraph beginning on page 171, line 2 as follows:

(2) The NTRU cryptosystem used in the present invention may be, instead of in the type described in the non-patent reference 3, in an EESS (efficient embedded security standard) type. The detail of the EESS-type NTRU cryptosystem is described in "EESS:Consortium for efficient embedded security, efficient embedded security standards #1: Implementation aspects of NTRU encrypt and NTRU sign, Version 2.0," ~~available at~~ ~~http://www.eeesstandards.org~~, May 2003. Therefore, the following only briefly discusses the EESS-type NTRU cryptosystem.